# TRADE SECRECY MEETS GENERATIVE AI

**CAMILLA A. HRDY**[1]

ABSTRACT

Generative AI models like ChatGPT raise novel issues for trade secret law. This Essay identifies three major developments and explains how the law will likely respond based on analogies to past technologies and past case law.

First, widespread use of generative AI poses new risks to companies' existing trade secrets. For example, trade secret owners' own employees might inadvertently share trade secrets with a generative AI tool like ChatGPT, which might disseminate this information to competitors or third parties. I argue this new disclosure risk, at the margins, raises the bar for keeping trade secrets. But companies will likely adapt their risk management strategies, as they did in the face of prior information-distribution technologies, such as the internet.

Second, generative AI will add to the universe of information that can be protected under trade secret law. Trade secret law will be available even for information that is not protected by patent and copyright law. Patent and copyright law have human creator requirements. But trade secret law has no human creator requirement. Therefore, purely AI-generated outputs that do not qualify for patent or copyright protection can be protected as trade secrets.

Third, companies that develop valuable new generative AI tools will be able to rely on trade secrecy to protect that technology, even when other forms of IP are unavailing. Trade secret law, especially when supplemented by restrictive contractual "terms of use," can protect various types of information related to generative AI, including information that does not qualify for copyright or patent protection.

Even though generative AI models will initially benefit from a combination of trade secrecy and contract protection, the models are highly vulnerable to "reverse engineering." For example, OpenAI, the maker of ChatGPT, recently accused the makers of the new AI model, "DeepSeek," of engaging in "knowledge distillation" to develop their competing system—using the larger, more complex, and more expensive ChatGPT model to build a smaller, simpler, and cheaper one. Trade secret law, although it generally permits reverse engineering, may not condone this conduct. Courts might construe these activities as a violation of contract law, since knowledge distillation seems to violate OpenAI's contractual terms of use; and courts might *also* view these activities as

[1] Associate Professor of Law, Rutgers Law School. Many thanks to Ryan Abbott, Jonas Anderson, Victoria Cundiff, Tait Graves, James Grimmelmann, Eric Goldman, Cynthia Ho, Sonia Katyal, Ed Lee, Mark Lemley, Dave Levine, Orly Lobel, Mike Madison, Tim Murphy, Elizabeth Rowe, Sharon Sandeen, Jake Sherkow, Deepa Varadarajan, John Villasenor, and participants at the 2024 Trade Secrets Virtual Workshop, Works in Progress in Intellectual Property (WIPIP) 2024 at Santa Clara Law, and the 2024 Symposium on AI Disrupting Law Symposium at Chicago-Kent College of Law. Thanks to Devin Owens, J.D. Candidate at Akron Law, for his research and ideas about "model extraction attacks."

a violation of federal and state trade secret law. In software cases, courts have held that using cutting-edge techniques like data scraping to access trade secrets constitutes acquisition by "improper means," and thus misappropriation, especially when contractual terms of use explicitly prohibit this conduct. The makers of DeepSeek claim they independently developed their model, but if this is not true, trade secret law could provide an avenue for legal liability.

## INTRODUCTION

This Essay addresses the major issues that generative artificial intelligence ("generative AI") raises for trade secret law.[2] Trade secret law is a form of intellectual property law that has existed for centuries. It is an important way that companies protect valuable, secret information. Today, trade secrets are protected both under federal law, through the Defend Trade Secrets Act (DTSA), and under state law. Most states have adopted some version of the Uniform Trade Secrets Act (UTSA).[3] A trade secret is defined by statute as "information"[4] that is not "generally known" or "readily ascertainable through proper means,"[5] that derives "independent economic value" from secrecy,[6] and that the putative owner has taken "reasonable measures" to keep secret.[7] Trade secret law protects trade secrets against two main types of "bad acts," called "misappropriation." First, trade secret law prohibits the use or disclosure of a trade secret by someone who received the information under a duty of confidentiality. Second, trade secret law prohibits the acquisition, use, or disclosure of a trade secret by someone who obtained the trade secret using "improper means," like spying, trespassing, or "hacking."[8] Trade secret law does not prohibit acquiring trade secrets through legal "reverse engineering"—that is, picking apart a publicly-available product to figure out how it works. [9]

Generative AI is a remarkable new form of artificial intelligence.[10] The most famous version of generative AI is ChatGPT, a large language model developed and distributed by

---

[2] This Essay was written for the 2024 "AI Disrupting Law" Symposium at Chicago-Kent College of Law. This essay is not, however, the first to address the implications of generative AI for trade secret law. *See* David S. Levine, *Generative Artificial Intelligence and Trade Secrecy*, 3 JOURNAL OF FREE SPEECH LAW 559 (2023). I discuss and build upon many of Dave Levine's insights in Part I of this Essay.

[3] *See generally* Camilla A. Hrdy & Mark Lemley, *Abandoning Trade Secrets*, 73 STAN. L. REV., 1, 15-25 (2021).

[4] 18 U.S.C. § 1839(3) (2016). *See also* Uniform Trade Secrets Act § 1 (1986) [hereinafter *UTSA*] (providing that potentially protectable "information," can include "a formula, pattern, compilation, program, device, method, technique, or process.").

[5] 18 U.S.C. § 1839(3)(B); UTSA § 1.

[6] 18 U.S.C. § 1839(3)(B); UTSA § 1. *See also* Camilla A. Hrdy, *The Value in Secrecy*, 91 FORDHAM L. REV. 557, 559, 568-76 (2022) (explaining various components of the modern independent economic value requirement).

[7] 18 U.S.C. § 1839(3)(A); UTSA § 1.

[8] 18 U.S.C. § 1839(5); UTSA § 1. *See also* Compulife Software, Inc. v. Newman, 111 F.4th 1147 (11th Cir. 2024) (affirming that using "data scraping" to acquire secret, economically valuable information from a website can constitute misappropriation of trade secrets).

[9] 18 U.S.C. § 1839(6); *see also* UTSA § 1, cmt.

[10] *See generally* Daryl Lim, *AI & IP: Innovation & Creativity in an Age of Accelerated Change*, 52 AKRON L. REV. 813 (2018); Charlotte Tschider, *Beyond the "Black Box"*, 98 DENVER L. REV. 683 (2021); Hon. Xavier Rodriguez, *Artificial Intelligence (AI) and the Practice of Law*, 24 SEDONA CONF. J. 783 (2023); Amy Winograd, *Loose Lipped Large Language Model Spill Your Secrets: The Privacy Implications of Large Language Models,* 36

OpenAI. ChatGPT has both extraordinary generative capabilities and a unique facility with human language. For most users, ChatGPT is an interactive "chatbot" accessed through a smartphone application or a web browser, which can instantly spit out responses to users' prompts. Generative AIs like ChatGPT are created by training algorithms on a very large universe of data called "training data." Generative AI algorithms use this data (the inputs) to generate new content that is similar to the training data, but is in fact newly-generated information (the outputs).[11] Through the training process, the algorithms learn and improve to the point that they function as truly creative sources of new information.

In this Essay, I discuss three novel issues that ChatGPT and similar generative AI technologies raise for trade secret law. In doing so, I identify analogies and case law from the past that might help assess how these issues will play out.

First, the widespread use of generative AI poses new risks to companies' *existing* trade secrets. To give just one example, trade secret owners' employees might inadvertently share trade secrets with a generative AI tool like ChatGPT. Assuming the model trains on that information, it might disclose it to third parties. This is indeed a new risk, but it's highly analogous to past situations in which a new technology threatened trade secrets. The main analogy that comes to mind is the internet. In the late 1990s, some commentators worried that the internet would spell the end of trade secrecy. It did not. Instead, the internet requires companies to adjust their trade secret management practices. I suspect the same will be the case with generative AI. At the same time, though, the standard for what can be a trade secret may get substantively higher. And that's probably a good thing. Too much low-value information can be protected through trade secret law, including old information that does not deserve to be protected. [12] That seems to be the most likely sort of information that ChatGPT could figure out.[13]

Second, generative AI will add to the universe of information that can be protected under trade secret law. Indeed, trade secret law may be available even for information that is *not* protected by patent and copyright law. Patent and copyright law have human creator requirements. But trade secret law has no human creator requirement. Therefore, purely AI-generated outputs that do not qualify for patent or copyright protection might be protectable as trade secrets. To support this

---

HARV. J.L. & TECH. L.J. 615 (2023); Ryan Abbott & Elizabeth Rothman, *Disrupting Creativity: Copyright Law in the Age of Generative Artificial Intelligence*, 75 FLA. L. REV. 1141 (2023); Gaetan de Rassenfosse et al., *AI-Generated Inventions: Implications for the Patent System*, 96 S. CAL. L. REV. 101 (2023); Maura Grossman et al., *The GPT Judge: Justice in a Generative AI World,* 23 DUKE L. & TECH. J. 1, 8 (forthcoming 2025) (available at https://ssrn.com/abstract=4460184); Katherine Lee et al., *Talkin' 'Bout AI Generation: Copyright and the Generative-AI Supply Chain*, J. COPYRIGHT SOC'Y (forthcoming 2025) (available at https://ssrn.com/abstract=4523551). *See also* Rebecca Heilweil, *What is Generative AI, and why is it Suddenly Everywhere? Between ChatGPT and Stable Diffusion, AI Suddenly Feels Mainstream,* VOX (Jan. 5, 2023, 8:00 AM) https://www.vox.com/recode/2023/1/5/23539055/generative-ai-chatgpt-stable-diffusion-lensa-dall-e [https://perma.cc/U6EH-BQXU]; Jacob Schneider, *Generative AI's Output: How Is It Created, and What IP Rights Should It Receive?* JD SUPRA (Oct. 3, 2023) https://www.jdsupra.com/legalnews/generative-ai-s-output-how-is-it-2360043/ [https://perma.cc/9MFZ-ZKNA].

[11] In this essay I use inputs to refer the information used to train generative AI models, and outputs to refer to the content that a generative AI model produces, often in response to human prompts. *C.f.* Mark Lemley & Bryan Casey, *Fair Learning,* 99 TEX. L. REV. 743, 777 (2020).

[12] *See generally* Hrdy & Lemley, *supra* note 3, at 1.

[13] *See infra* Part I.

thesis, I point both to the text of the trade secret statutes and the history of trade secret law. Historically, most trade secrets have not been created by the same entity that owns them. Trade secrets are created by people—employees or independent contractors—who are hired by the entity that ends up owning the trade secrets. By analogy, AI-generated trade secrets will be owned by the entity that owns the AI or its licensees and assignees.[14]

Third, companies that develop valuable new generative AI tools will be able to rely on trade secrecy to protect that technology. Precisely how trade secrecy applies to generative AI—and AI generally—is complex.[15] In this Essay, I provide a broad overview. I identify the types of information related to generative AI that might qualify as trade secrets. I explain why patent and copyright law are insufficient for protecting these types of information. I show that trade secret law provides an alternative, even for generative AI models that are distributed to the general public. The major caveat is the risk of "reverse engineering"—that is, the risk that other actors will learn how to replicate a generative AI model by inspecting the publicly-distributed version. However, I argue that, for better or worse, courts are likely to follow precedents involving traditional software, in which courts found that acts which resembled lawful reverse engineering were in fact acquisition of trade secrets by "improper means," both due to the nature of the methods utilized, and due to the fact that the software was released under "terms of use" that prohibited reverse engineering. As a result, generative AI models can be protected using a combination of trade secrecy and contract protection.[16]

I now proceed in three parts, discussing each of these three issues in detail, drawing on statutes and case law from prior technologies to predict how the law will address these novel issues.

## I. GENERATIVE AI CAN THREATEN COMPANIES' EXISTING TRADE SECRETS

The "hottest" topic among trade secret practitioners is the sudden risk that generative AI tools, like ChatGPT, apparently pose to companies' existing trade secrets. The basic concern is that, due to generative AI, some former trade secrets may be rendered "generally known" or "readily ascertainable,"[17] and thus no longer protectable under the trade secret statutes. This can happen *purely at a technological level*. Without anyone intending for it to happen, generative AI might suddenly wipe out a subset of intellectual property merely by existing.[18]

In this part, I explain how this can happen in various circumstances. In doing so, I draw and build upon David Levine's observations in his insightful essay, *Generative Artificial Intelligence and Trade Secrecy*. Levine argues that generative AI can act as a "mundane destroyer"

---

[14] *See infra* Part II.

[15] *See* Camilla A. Hrdy. *Keeping ChatGPT a Trade Secret While Selling It Too*, BERKELEY TECH. L.J. (forthcoming 2025), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4879849

[16] *See infra* Part III.

[17] 18 U.S.C. § 1839(3)(B); UTSA § 1.

[18] Jake Sherkow has recently discussed a somewhat analogous situation of technology-driven trade secret destruction in his new article arguing that advances in technology have made DNA sequences readily ascertainable. According to Sherkow, "advances in and the democratization of DNA sequencing technology, *independent of any act on the part of DNA sequence data owners*, have diminished the trade secret protectability of DNA sequence information." *See* Jacob S. Sherkow, *The Myth of DNA Trade Secrecy,* 75 HASTINGS L.J. (forthcoming 2024).

of trade secrets.[19] I use that same general framework here, considering precisely how generative AI can act as Levine's "mundane destroyer" of trade secrets.

### *A. Company employees who use generative AI may inadvertently disclose trade secrets.*

The most basic way generative AI can destroy trade secrets is that company employees will use generative AI and inadvertently disclose company trade secrets when prompting the model. Assuming generative AI trains on that information and incorporates it into responses it gives to third parties, this can destroy the information's trade secret status.[20]

Doctrinally, destruction occurs for three reasons. First, the information has become "generally known" or "readily ascertainable" to others who can easily access it using "proper means."[21] Information is deemed "readily ascertainable" if it can easily be discovered by reviewing widely available sources, such as patents, "trade journals, reference books, or published materials," or if it can easily be copied from a product that is "available on the market."[22] Courts will likely place generative AI on the same footing as these traditional sources. That is what courts have done with the internet. Releasing trade secrets on the internet is akin to releasing trade secrets in a patent, book, or trade journal. Posting trade secrets on the internet renders trade secrets "generally available to the public."[23] Therefore, if it is easy to discern information by prompting a widely-available generative AI tool, this should render the information generally known or readily ascertainable, and thus not a trade secret.

Second, information that can easily be extracted from a generative AI model through common-sense prompts no longer derives "independent economic value" due to being kept secret. Even if the information still has "value" in some abstract sense—for example, because it was costly to develop—trade secret law does not care about "value" in the abstract. It only cares about the value caused by secrecy.[24] If any user can theoretically prompt a generative AI tool to reveal, say, the formula for a pharmaceutical drug, then that formula is not economically valuable as a result of secrecy, no matter how expensive it was to develop.

---

[19] Levine, *supra* note 2*,* at 575.

[20] Levine, *supra* note 2*,* at 578 (asserting that it is "easy for ChatGPT to share information with a third party that in- corporates input by a trade secret holder . . . . "). *See also, id*. at 580 ("[B]ecause trade secret information can be found in hidden corners of the internet, and not easily found even by search engines, it is conceivable that the extraneous and obscure accidental disclosure could come back to haunt trade secret holders through speech generated by ChatGPT, based upon a third-party's prompt.").

[21] As discussed in the next section, one could argue in some circumstances that using ChatGPT is an "improper means" of accessing trade secrets, which would make this information *not* readily ascertainable using "proper means" as the statutes require.

[22] The UTSA commentary states, in relevant part: "Information is readily ascertainable if it is available in trade journals, reference books, or published materials. Often, the nature of a product lends itself to being readily copied as soon as it is available on the market. On the other hand, if reverse engineering is lengthy and expensive, a person who discovers the trade secret through reverse engineering can have a trade secret in the information obtained from reverse engineering." *See* UTSA, § 1, cmt.

[23] *See, e.g.,* Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 923 F. Supp. 1231, 1256 (N.D. Cal. 1995) ("[O]ne of the Internet's virtues, that it gives even the poorest individuals the power to publish to millions of readers … Although a work posted to an Internet newsgroup remains accessible to the public for only a limited amount of time, once that trade secret has been released into the public domain there is no retrieving it.").

[24] *See also* Hrdy, *supra* 6, at 595-99 (discussing requirement that value be "caused by" secrecy).

Third, a company that continues to use, or allow its employees to use, generative AI tools, *despite the risk of leakage*, has failed to take "reasonable" measures to maintain the information's secrecy. To quote Levine, "if a trade secret owner places confidential information into ChatGPT's training data (wittingly or unwittingly) through a query or some other action, that could deviate sufficiently from 'reasonable efforts' to maintain a trade secret as to vitiate trade secret protection all together."[25] The analogy that courts sometimes use is "abandonment" or "forfeiture." If a trade secret owner allows its workers to keep using generative AI tools, knowing that each use poses a significant risk of leaking trade secrets, it is as if the trade secret owner has willingly "abandoned," or "forfeited," its property. Anyone who wishes to use this abandoned property thereafter is entitled to do so.[26]

### *B. Generative AI and Trade Secret Management: The New Internet?*

This novel, employee-driven risk to trade secrets sounds like a big deal. Soon after ChatGPT became available, many companies and law firms responded by banning or restricting employees' access to ChatGPT, due to concerns over trade secrets and private information.[27] But I am skeptical that this is really doomsday. This is not the first time a new technology has made it easier to disclose trade secrets.

Commentators voiced the same worry when the internet was created. In the 1990s, courts quickly concluded that the release of trade secrets on the internet generally destroys trade secrecy status. "Although the Internet is a new technology," one court wrote in 1995, "it requires no great leap to conclude that because more than 25 million people" can access the internet, trade secrets revealed in works posted on the internet "lose their status as secrets" because they become "generally known" to all the relevant people.[28] Back then, as today, commentators questioned whether trade secrecy could survive. Given that literally anyone could access information on the internet, surely, more and more information would be found to be generally known or readily ascertainable through proper means.[29]

---

[25] Levine, *supra* note 2, at 564.

[26] *See* Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 179 (7th Cir. 1991) (stating that a trade secret that is not the subject of "reasonable" measures to retain secrecy is like "abandoned property…[A] defendant is perfectly entitled to obtain the property if the plaintiff has abandoned it by giving it away without restrictions."). *See also, e.g.,* Deepa Varadarajan, *Trade Secret Precautions, Possession, and Notice,* 68 HASTINGS L. J. 357, (2017) (noting analogy between failure to take reasonable steps to preserve secrecy and trademark "abandonment"); Deepa Varadarajan, *Forfeiting IP*, 59 AM. BUS. L. J. 175, 175 (2022) (arguing that failure to take reasonable steps to preserve secrecy is akin to "forfeiture").

[27] JONES DAY, *Trade Secrets and Generative AI: Protective Measures In an Evolving Technological Landscape*, (June 9, 2023), https://www.jonesday.com/en/insights/2023/06/trade-secrets-and-generative-ai [https://perma.cc/QW3B-NJA3]; Joshua Weigensberg & Kate Garber, *Risks That Generative AI Poses to Trade Secret Protections*, N.Y. LAW J. (June 13, 2023), https://www.pryorcashman.com/publications/risks-that-generative-ai-poses-to-trade-secret-protections [https://perma.cc/BS9Q-2TLD].

[28] Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 923 F. Supp. 1231, 1256 (N.D. Cal. 1995).

[29] As one commentator put it, "[s]ince more information is available," in light of the internet, "the general knowledge of the industry may expand, thus making it more difficult for a trade secret owner to show that his secret information was not generally known." David G. Majdali, *Trade Secrets Versus the Internet: Can Trade Secret Protection Survive in the Internet Age?*, 22 WHITTIER L. REV. 125, 144-45 (2000).

But the issue quickly became one of trade secret management. The protection measures required to retain trade secrecy had changed; the standard for what level of protection was "reasonable" in light of the costs, benefits, and risks had risen. Companies had to expend new resources implementing all of the emerging digital protection measures, like password protections, firewalls, and encryptions. They had to spend more time monitoring employees' internet activities. And, of course, they turned more and more to contracts, such as confidentiality provisions and end user license agreements (EULAs), to ensure that their information was difficult to share or access without breaching a contract.[30]

The same is likely to be true today. To channel Elizabeth Rower, new technological risks—whether it's the internet or pervasive use of generative AI—necessarily place a "higher duty of care on trade secret owners"; they will have to do more to protect their information against the new yet highly "foreseeable" risk that their employees will use generative AI.[31] The requisite trade secrecy management protocols will change in response, and with that, costs might initially rise.

This raises questions about how exactly companies should adapt in the face of generative AI tools and what they should do to protect their secrets. I am certainly not going to attempt to give a full menu here. At a high level, it seems clear that companies will have to be strategic about what they let their workers do with generative AI. One option is a full ban on employees using generative AI, as some companies have done. But this is not realistic. Workers will likely deviate from the rule or just go home and use generative AI off the clock.

A more realistic response is to give workers the option to use an in-house model or alternatively obtain an "Enterprise License" for an off-the-shelf model. These Enterprise Licenses come with additional confidentiality and privacy restrictions. For example, OpenAI now offers an Enterprise License that permits licensees to incorporate ChatGPT into their own businesses or applications under specific terms and that includes a more robust confidentiality provision.[32] The "Business Terms," which governs the ChatGPT Enterprise License, provides in relevant part that "Customer Content" (inputs and outputs to ChatGPT) will be treated as "Confidential Information," and that OpenAI will "(a) only use [the Enterprise Licensee's] Confidential Information to exercise its rights and fulfill its obligations under this Agreement, (b) take reasonable measures to protect the Confidential Information, and (c) not disclose the Confidential Information to any third party except as expressly permitted in this Agreement."[33]

This could provide some assurance for companies that adopt an Enterprise License for ChatGPT in the workplace. But what if employees go home and use the general-purpose, publicly available ChatGPT model off the clock? There is extraordinary risk here because the individual Terms of Use for ChatGPT *contain no confidentiality provision at all*, thus permitting ChatGPT

---

[30] *Id.* at 145-56.

[31] Elizabeth A. Rowe, *Contributory Negligence, Technology, and Trade Secrets*, 17 GEO. MASON L. REV. 1, 3 (2009).

[32] OPENAI, *Business Enterprise*, https://openai.com/enterprise [https://perma.cc/4S5J-AYHK]. *See also* Sachin Bhatmuley et al., *Generative AI End-User License Agreements: What Users Need to Know*, JDSUPRA, (Aug. 7, 2023) https://www.jdsupra.com/legalnews/generative-ai-end-user-license-3308704/ [https://perma.cc/9LPE-TNN2].

[33] OPENAI, *Business Terms*, https://openai.com/policies/business-terms [https://perma.cc/4NSS-XXYV].

to train on any inputs it receives, all else being equal.[34] That said, OpenAI has also recently adopted new Terms of Use for *individual* ChatGPT users. These Terms of Use give individual users the option to "opt out" of having their content trained on by the ChatGPT model. The new Terms of Use, effective January 31, 2024 states:

> "Opt Out. If you do not want us to use your Content to train our models, you can opt out by following the instructions in this Help Center article. Please note that in some cases this may limit the ability of our Services to better address your specific use case."[35]

One thing risk-adverse companies could do, then, is require all their employees to exercise the opt-out option any time they use ChatGPT. Still, these sorts of assurances from third-party AI developers are unlikely to provide sufficient protection for the company's information. I predict that at least some companies will start by licensing off-the-shelf models like ChatGPT, relying on contractual assurances of confidentiality, but will eventually develop *their own in-house models.* In-house models would be far easier to control. Companies could adopt their own information security precautions. They could also keep the AI itself, and the AI's outputs, as trade secrets. I will discuss these issues in the next parts.

### *C. Deliberate Use of Generative AI to Discover Trade Secrets*

So far, I've discussed how generative AI can contribute to inadvertent trade secret destruction, like when company employees may inadvertently leak trade secrets to generative AI while prompting the model. But generative AI can also expose trade secrets when a user deliberately attempts to figure out trade secrets.[36] Levine identifies this issue as well, arguing that ChatGPT can serve as a "very capable partner in crime . . . ."[37] For example, imagine that a ChatGPT user—suspecting that a model has been trained on a competitor's trade secret information—deliberately prompts ChatGPT to reveal those secrets in outputs.

In this situation, where the prompting is done deliberately and with the intent to learn another's trade secrets, it is possible these activities will themselves violate trade secret law. But it's not clear that they do. On the one hand, trade secret owners can argue this activity constitutes "misappropriation" of trade secrets, and that the strategic prompter should be liable under trade

---

[34] OPENAI, *Terms of Use*, https://openai.com/policies/terms-of-use [https://perma.cc/Z49Q-GE52].

[35] *Id.*

[36] Jim Chilton, *The New Risks ChatGPT Poses to Cybersecurity*, HARV. BUS. REV.: CYBERSECURITY AND DIGITAL PRIVACY, (April 21, 2023), https://hbr.org/2023/04/the-new-risks-chatgpt-poses-to-cybersecurity#:~:text=While%20there's%20significant%20discussion%20around,and%20designed%20to%20be%2C%20impartial [https://perma.cc/PLE4-33EQ].

[37] Levine, *supra* note 2, at 564 ("ChatGPT can aid in the misappropriation of a trade secret, acting as an accomplice or agent (of sorts) of a trade secret misappropriator. If ChatGPT is directed to answer a query through prompts that could reveal a trade secret from within its own universe of data, the clever trade secret misappropriator has found a very capable partner in crime.").

secret law, as well as under the Computer Fraud and Abuse Act or other statutes.[38] On the other hand, the defendant can argue that using generative AI to discern another's trade secrets is nothing more than legal competitive intelligence and that use of generative AI is akin to legal reverse engineering; it's like picking apart a product to figure out another's trade secrets.[39]

Whether using generative AI to discern another's trade secrets constitutes "improper means" is a fact-intensive inquiry. In civil cases, courts have looked both at the perceived social "wrongness" of a defendant's actions and at the degree to which the defendant's success in accessing trade secrets was precipitated by the trade secret holder's own failure to protect against this sort of act.[40] Over the decades, courts have found a wide variety of actions to be "improper," ranging from flying a plane over an unfinished plant to hiring detectives to rummage through garbage.[41] But other actions, such as picking locks to learn lock codes, have been found to be lawful "reverse engineering."[42]

A recent Eleventh Circuit case, *Compulife Software Inc. v. Newman*, suggests that courts may view using generative AI to discern trade secrets as an "improper means" of acquisition. In *Compulife*, the defendants hired a woman named Natal (whom the court called a "hacker"[43]) to obtain access to a database of insurance quotes "by creating a robot" to "scrape" the plaintiff's website.[44] The lower court, via a magistrate judge, held the defendants' actions were legal, given that the website was made "freely available to the public."[45]

The Eleventh Circuit reversed, holding the lower court failed to consider whether the method the defendants used to obtain the database was "improper means." The Eleventh Circuit emphasized the *non-human* nature of the method that the defendants used to obtain trade secrets. "[T]he true power of a scraping attack," the court wrote, "is realized by creating a robot … that

---

[38] *See generally* Hasala Ariyaratne, *The Impact of ChatGPT on Cybercrime and Why Existing Criminal Laws Are Adequate,* 60 AM. CRIM. L. REV 1 (2023) (discussing other causes of action that could arise from the use of ChatGPT in conducting "cybercrimes," including hacking, which might already be criminalized by the federal Computer Fraud and Abuse Act ("CFAA")).

[39] *See* ELIZABETH ROWE & SHARON SANDEEN, CASES AND MATERIALS ON TRADE SECRETS 230-231 (2012) (observing that competitive intelligence is "legal and ethical," but can sometimes "cross the line into trade secret misappropriation."). I discuss "reverse engineering" further in Part III.

[40] Restatement (Third) of Unfair Competition § 43 cmt. c (Am. L. Inst. 1995).

[41] *See* Victoria A. Cundiff, *Reverse Engineering the Competition,* paper presented at L. SEMINARS INT'L PROGRAM ON TRADE SECRETS (2003) (on file with the author) (citing, e.g., E.I. DuPont de Nemours & Co., Inc. v. Christopher, 431 F.2d 1012 (5th Cir. 1970); Tennant Co. v. Advance Machine Co., Inc., 355 N.W.2d 720, 725 (Minn. Ct. App. 1984)).

[42] Chicago Lock Co. v. Fanberg, 676 F.2d 400, 404 (9th Cir. 1982) (holding it was not improper means to publish key codes to locks obtained from "comparatively small" number of locksmiths who supplied this information because this was "proper reverse engineering.").

[43] Hacking is the "act of identifying and then exploiting weaknesses in a computer system or network, usually to gain unauthorized access to personal or organizational data." The Federal Computer Fraud and Abuse Act ("CFAA") criminalizes hacking. Hasala Ariyaratne, *The Impact of ChatGPT on Cybercrime and Why Existing Criminal Laws Are Adequate,* 60 AM. CRIM. L. REV. 1, (2023).

[44] Compulife Software Inc. v. Newman, 959 F.3d 1288, 1298-1300 (11th Cir. 2020).

[45] *Id*. at 1312-1314.

can make many requests automatically and much more rapidly than any human could."[46] The Eleventh Circuit remanded for the lower court to determine whether the "scraping attack" amounted to improper means.[47] On remand, the lower court held in favor of the plaintiff after a bench trial. The court held that the defendants acquired plaintiff's trade secrets using "improper means" by "using a robot to hack" the plaintiff's website.[48] The Eleventh Circuit affirmed.[49] One of the defendants has filed a petition for certiorari to the U.S. Supreme Court.[50] The Court has not yet reached a decision on whether to grant certiorari.

Courts might consider use of generative AI to discern another's trade secrets as akin to the automated methods used in *Compulife*. Generative AI can enhance humans' capacity to learn trade secrets, and go beyond what would ordinarily be expected. A court might decide that using such non-human means to access trade secrets is "improper means."

This argument will be even stronger given that the contracts governing how users employ generative AI models typically contractually prohibit using the models "in a way that infringes, misappropriates or violates anyone's rights."[51] As discussed in Part III, contracts play an important role in defining what constitutes "improper means" of acquiring trade secrets. Thus, if a "terms of use" makes plain that users cannot use the generative AI to discern others' trade secrets, a court will almost certainly take this into account in deciding whether the action is "improper." Put differently, when generative AI companies like OpenAI prohibit using their models to discern trade secrets, this helps ensure that using generative AI to discern trade secrets will be deemed illegal under trade secret law.

### *D. "Is Everything Readily Ascertainable?"*

The final risk generative AI poses to existing trade secrets is far more apocalyptic and may, in fact, be insurmountable because it's outside of companies' control. What if generative AI models get so good at searching available data and piecing together information that they can figure out companies' trade secrets—even *without* being fed inside information, and even *without* "bad actors" making deliberate attempts to discover trade secrets? Could that render companies' trade secrets suddenly "readily ascertainable"?

For example, consider a company, such as Coca-Cola, which has a long-standing trade secret in the formula needed to reproduce its famous soft drink. Then, imagine that a generative AI model is developed that is *so powerful* that it can piece together exactly what this formula is.

---

46 *Id*. at 1299; *see also id. at* 1314 ("[W]hile manually accessing quotes from Compulife's database is unlikely ever to constitute improper means, using a bot to collect an otherwise infeasible amount of data may well be—in the same way that using aerial photography may be improper when a secret is exposed to view from above.") (citing E. I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1013 (5th Cir. 1970)).

47 *Id*. at 1313.

48. *See* Compulife Software, Inc. v. Rutstein, No. 9:16-CV-80808, 2021 WL 3713173, at *21 (S.D. Fla. July 12, 2021), order clarified, No. 9:16-CV-80808-BER, 2021 WL 5830554 (S.D. Fla. Oct. 20, 2021).

49. *See* Compulife Software, Inc. v. Newman, 111 F.4th 1147, 1162-1163 (11th Cir. 2024).

50. *See* Petition for Writ of Certiorari, Compulife Software Inc. v. Newman, No. 24-634 (U.S. Nov. 27, 2024).

51 *Terms of Use*, *supra* note 30.

Now, *anyone* using only common-sense prompts can figure out the formula for Coke. Would this render the Coca-Cola trade secret "readily ascertainable" through proper means?

This problem is similar to the "everything is obvious" problem that scholars like Ryan Abbott have discussed in patent law. To be eligible for a patent, an invention must not be "obvious" to be patentable. Obviousness is judged from the perspective of a hypothetical "person having ordinary skill in the art" (PHOSITA). If artificial intelligence can be considered in judging whether an invention is obvious, then more and more inventions might become obvious and thus unpatentable as artificial intelligence improves.[52]

Just as some scholars worry about whether "everything is obvious" in light of machine intelligence, so too in trade secret law we might worry that "everything is readily ascertainable." In fact, I think this concern is *even more severe* in trade secret law than in patent law. Patent law has always set a high obviousness bar because the hypothetical PHOSITA is assumed to have access to all publicly available prior art. Trade secret law tends to be less strict in this regard because it asks whether the asserted trade secret information is, *in reality*, generally known or readily ascertainable to others in the industry.[53] This means the sudden availability of an AI entity—which can be used by people in the industry as well as by the general public—could truly raise the bar for what can be a trade secret. If everyone can use generative AI to figure out a putative trade secret by entering "common-sense prompts," that information should, in theory, be deemed generally known or at least readily ascertainable.[54] The Coca-Cola formula that was a trade secret yesterday might become generally known or readily ascertainable as soon as the all-powerful AI hits the market.

As mentioned above, the internet analogy comes instantly to mind. People thought the internet would destroy trade secrets, but instead, it just raised the cost of protecting them. That said, I do not think the internet analogy solves the "everything is readily ascertainable" problem. The internet does not generate. The internet cannot, on its own, piece together all of these disparate

---

[52] As Abbot puts it, "[t]he nonobviousness bar will continue to rise as machines inevitably become increasingly sophisticated. Taken to its logical extreme, and given there may be no limit to how intelligent computers will become, it may be that every invention will one day be obvious to commonly used computers. That would mean no more patents should be issued without some radical change to current patentability criteria." Ryan Abbott, *Everything Is Obvious*, 66 UCLA L. Rev. 2, 8 (2019). *See also* Liza Vertinsky, *Thinking Machines and Patent Law*, *in* RESEARCH HANDBOOK OF ARTIFICIAL INTELLIGENCE (Woodrow Barfield ed. 2018) (arguing that "[w]ith thinking machines in the equation . . . policymakers might have to consider whether the PHOSITA should be modified to include thinking machines – perhaps some kind of machine/person combination or "M/PHOSITA." But if thinking machines were to be included in the analysis as part of the PHOSITA category, it would be difficult if not almost impossible to limit the expansiveness of non-obviousness determinations.") (quote at p. 15 of the electronic copy, available at https://ssrn.com/abstract=3036030).

[53] *See* Camilla Hrdy & Sharon Sandeen, *The Trade Secrecy Standard for Patent Prior Art*, 70 AM. U. L. REV. 1269 (2021) (discussing trade secret law's generally known or readily ascertainable standards).

[54] *See* Brandi B. Balanda, *Protecting Trade Secrets in the Era of Generative Artificial Intelligence*, SAVITT, BRUCE, & WILEY (June 9, 2023), https://web.archive.org/web/20230929043718/https://www.sbwllp.com/protecting-trade-secrets-in-the-era-of-generative-artificial-intelligence-part-ii-novelty/ [https://perma.cc/5CT5-HH54?type=image] (observing that AI tools "could potentially generate ideas for products and strategies similar to those humans might otherwise conceive[,]" but noting that this presents a trade secrecy "challenge for businesses" because how can they "prove their product feature, strategy plan, formula or methodology" is a trade secret "when it can be replicated by AI through common-sense prompts?").

data points to discern trade secrets. So I think this really is a new risk. The bar *will* likely go up for what can be a trade secret. Information that can easily be figured out by anyone entering common-sense prompts into an AI will not be protected as a trade secret. It will be deemed to be readily ascertainable or to lack economic value as a result of being kept secret.

However, I think this is probably a very good thing. As I have previously argued, trade secret law currently protects far too much information, including low-value information, non-economic information, expired information, and information whose value does not stem from secrecy.[55] I think trade secret law would, overall, benefit from raising the bar on what can be a trade secret. Widespread use of generative AI would do that by making it harder to keep information legally secret. This would whittle down the universe of trade secrets to reflect only those with true value.[56]

## II. TRADE SECRET LAW CAN PROTECT GENERATIVE AI OUTPUTS

The second novel issue that generative AI raises for trade secret law is the prospect of trade secrecy protection AI-generated information. At present, a purely AI-generated output cannot be protected using either patent or copyright law to the extent that there is no identifiable human inventor or author.[57] But these outputs might be protected under trade secret law. David Levine, for instance, asserts that "generative AI creates a new and groundbreaking mechanism for not only trade secret dissemination, but also trade secret creation."[58] He argues that "[d]epending on how that information is viewed, managed, and used, these [outputs] could be potential new trade secrets[.]"[59]

In this part, I closely examine this proposition by asking: Can outputs of generative AI be protected under trade secret law, even if no human was involved in creating the outputs? For example, if a company develops an AI tool, and the AI creates trade secrets without any other human input, can the company claim ownership of those trade secrets? This is a novel question of law. But as I will explain below, a look at the statutes and history of trade secret law suggests that

---

[55] Hrdy, *supra* note 6, at 562-63 (discussing "value failures" including amount failures, type failures, timing failures, and causation failures).

[56] *Id*. at 564-65.

[57] *See* Thaler v. Vidal, 43 F.4th 1207 (Fed. Cir. 2022) (affirming that only natural persons can be named inventors on U.S. patents). *See also, e.g.,* Ryan Abbott, *Artificial Intelligence and Intellectual Property: An Introduction, in* RESEARCH HANDBOOK ON INTELLECTUAL PROPERTY AND ARTIFICIAL INTELLIGENCE 442–59 (Abbott, ed., 2022); Carys Craig, *The AI-Copyright Challenge: Tech-Neutraliy, Authorship, and the Public Interest*, *in* RESEARCH HANDBOOK ON INTELLECTUAL PROPERTY AND ARTIFICIAL INTELLIGENCE 442–59 (Abbott, ed., 2022) (discussing issue of AI authorship for copyright purposes). Inventions developed by humans with the help of AI may still be patentable, especially if humans are also involved in developing the AI system. *See* U.S. PATENT & TRADEMARK OFFICE, PUBLIC VIEWS ON ARTIFICIAL INTELLIGENCE AND INTELLECTUAL PROPERTY POLICY, 2-3, (Oct. 2020), https://www.uspto.gov/sites/default/files/documents/USPTO_AI-Report_2020-10-07.pdf [https://perma.cc/BM3U-5JWP] [hereinafter *USPTO VIEWS*]. Recently, the patent office has suggested a "joint inventorship" standard, asking whether a human is involved who would qualify as a joint inventor. *See* Denis Crouch, *Joint Inventorship: AI-Human Style,* PATENTLY-O, (Feb. 12, 2024), https://patentlyo.com/patent/2024/02/joint-inventorship-human.html#:~:text=No%20AI%20Inventors%20Allowed&text=4th%201207%20(Fed.,in%20developing%20the%20claimed%20invention [https://perma.cc/BY2U-DCN9].

[58] Levine, *supra* note 2*,* at 571.

[59] *Id.* at 568.

the answer is a resounding "yes." The lack of a human inventor is not dispositive in trade secret law in the same way that it is in patent and copyright law. Trade secrecy can protect AI-generated information just as comfortably as trade secrecy can protect human-generated information.

### *A. Trade Secrets are not Limited to Human Creators*

There are several reasons to conclude that AI-generated information can be protected under trade secret law, even if no humans are involved in the creation of the information.

First, trade secret law does not have—and never has had—any express human creator requirement. As John Villasenor writes, neither federal trade secret law nor state trade secret law provides any "affirmative requirement" that the entity that created a trade secret be a human.[60] At the federal level, the Defend Trade Secrets Act (DTSA), passed in 2016, specifically defines the "owner" of a trade secret as "the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed . . . ."[61] This indicates that the "owner" of a trade secret need not be the same entity that created it, and that the creator of the trade secret need not be a human being. To quote trade secret practitioners Erik Weibust and Dean Pelletier, this provision strongly supports the "DTSA's neutrality on who or what invents, develops, or generates information."[62]

Second, trade secret law's "standing" doctrines—which have been applied to determine who can sue to protect trade secrets under the common law and under state statutes adopting the Uniform Trade Secrets Act—generally give standing to sue to the person or entity that has "*possession*" of the trade secret and taken "reasonable security measures" to keep the information *secret*.[63] This suggests that a party can sue to protect a trade secret so long as the party possesses the information and takes reasonable steps to protect it, irrespective of whether the company developed the trade secret and whether the information was human-created.

Finally, most trade secret cases historically have involved employee-generated information owned by employers. It is well-established that employee-generated information is not necessarily owned by the employee herself. Rather, employee-generated information is usually owned by the employer. While the ownership rules in trade secret law have evolved over time, the modern trend shifts ownership of employee inventions to employers. This usually occurs through assignment agreements in employment contracts but could also occur in the absence of a contract if the employee is "hired to invent."[64] By analogy, if a machine owned by a company derives a new invention, then the company that owns the machine should own the invention.

---

[60] John Villasenor, *Artificial Intelligence, Trade Secrets, and the Challenge of Transparency*, 25 N.C. J.L. & TECH. 495, 507 (2024).

[61] *See* 18 U.S.C. § 1839(4) (2016).

[62] *See* Erik Weibust & Dean Pelletier, *Protecting AI-Generated Inventions as Trade Secrets Requires Protecting the Generative AI as Well*, IP WATCHDOG (July 24, 2022, 12:15 PM), https://ipwatchdog.com/2022/07/24/protecting-ai-generated-inventions-trade-secrets-requires-protecting-generative-ai-well/id=150372/ [https://perma.cc/23TT-A8V4].

[63] *See* Tait Graves, *Curiosities of Standing in Trade Secret Law,* 20 NW. J. TECH. & INTELL. PROP. 159, 159 (2023).

[64] *See* Catherine Fisk, *Removing the 'Fuel of Interest' from the 'Fire of Genius': Law and the Employee-Inventor, 1830-1930*, 65 U. CHI. L. REV. 1127, 1132 (1998).

The upshot of these arguments is that, yes, AI-generated information can be protectable as trade secrets. AI-generated information can be owned by the entity that owns the AI or by whichever entity obtains legal title to the trade secret, such as a license. An entity that possesses an AI-generated trade secret can have standing to protect that trade secret in court. It is even theoretically possible that an AI *itself* could one day develop, protect, and own its own trade secrets. In his new essay, *Do Androids Dream of Electric Incentives?*, Tim Murphy creatively explores how trade secret law doctrine and theory might apply in a future world where AI is so advanced that it can create, commercialize, and protect its own trade secrets.[65]

### *B. AI-Generated Trade Secrets May Be Easier to Protect than Human-Generated Trade Secrets*

So, AI-generated trade secrets may be protected similarly to employee-generated trade secrets. But this is not a direct analogy. One important difference is that AIs do not have "general knowledge, skill, and experience" that they can take away with them. Human workers generally pose a risk to their employers' trade secrets because they tend to depart and share trade secrets or their unprotectable "general knowledge skill and experience" with competitors. Human employees can always claim that some information they obtained on the job is their own unprotectable "general knowledge, skill, and experience," and not their employer's trade secrets.[66] But AI cannot do this. There is no precedent for AI maintaining "general knowledge, skill, and experience" as their own.

As a result, Jeanne Fromer has argued that increased use of AI to perform tasks previously done by human workers could actually make trade secrecy *easier* to maintain. Whereas departing human workers can bring their general knowledge, skill, and experience with them when they leave, "a machine performing this employee's task would never do so."[67] Machines

> will never take their general knowledge and skill elsewhere to competitors. Thus, by decreasing the number of employees that might carry their general knowledge and skill to new jobs and in any event the amount of knowledge and skill that each employee might have to take, increasing automation undermines a critical limitation on trade secrecy protection.[68]

This suggests that by delegating tasks to AI that were previously done by human workers, companies might be able to reduce the risk of leaks and retain trade secrecy protection for longer.

---

[65] *See* Tim Murphy, *Do Androids Dream of Electric Incentives?* AKRON L. REV. (forthcoming 2024) (initial draft on file with the author) (exploring how trade secret law theory would apply to artificial intelligence that creates new potential trade secrets).

[66] *See* Camilla A. Hrdy, *The General Knowledge, Skill, And Experience Paradox*, 60 B.C. L. REV. 2409, 2409 (2019) (arguing that departing employees can leave and use general knowledge skill experience that does not qualify as a trade secret in new endeavors).

[67] Jeanne Fromer, *Machines as the New Oompa Loompas*, 94 N.Y.U. L. REV. 706, 725 (2019).

[68] *Id.* at 725-26.

### *C. AI-generated trade secrets could be uniquely vulnerable to being deemed "readily ascertainable."*

There is an important caveat. It is certainly true that AI-generated information can be protected as trade secrets. It is also possible, as Jeanne Fromer argues, that preserving AI-generated information's trade secrecy status might be easier when companies adopt AIs for use in their business to perform tasks previously done by humans. However, at the same time, companies that wish to keep AI-generated information as trade secrets also face the challenge that I discussed above: The risk that their information will be deemed readily ascertainable. If the generative AI tool that created the information is available on the *open market* and is simultaneously being used by *others*, then those AI-generated outputs might be at risk of becoming generally known or at least readily ascertainable.

As explained above in Part I, trade secret law does not protect information after it has become readily ascertainable to others to whom it might be economically valuable. As Erik Weibust and Dean Pelletier astutely observe, this creates a risk to trade secrecy protection for AI-generated information in situations where the AI tool itself is not being used only in-house and is not protected as a trade secret. "[I]f the generative AI is not itself protected as a trade secret," they write, "then [the AI] may be vulnerable to . . . copying or reverse engineering. If the AI is copied or reverse engineered, then an invention or other information generated by the AI may be readily ascertainable through proper means and thus not be a trade secret . . . ."[69] Any protection afforded an "AI-generated invention" made by a "readily ascertainable" AI model would "be non-existent or fleeting."[70]

Weibust and Pelletier argue that the solution is to keep the generative AI as a trade secret, too. I discuss this issue below, considering whether it is possible to protect generative AI technology itself as a trade secret. However, this solution would *not* solve the problem of information developed using publicly available generative AI. If someone comes up with an invention using the latest subscription model of ChatGPT, for example, assuming their prompts are replicable by other people pursuing the same line of inquiry, that information would be readily ascertainable. It would not matter that OpenAI claims ChatGPT's underlying technology as its trade secret.

## III. PROTECTING GENERATIVE AI UNDER TRADE SECRET LAW

I have now discussed two novel issues that generative AI raises for trade secret law: the new risks generative AI poses to companies' existing trade secrets and the new potential for trade secret law to protect AI-generated information. I now turn to the final issue: Can generative AI's themselves be protected under trade secret law? Can popular AI tools like ChatGPT be kept as "trade secrets," even though they are marketed to the general public?[71] I discuss these issues here. I start below by identifying which features of a generative AI are likely to qualify as trade secrets

---

[69] Weibust & Pelletier, *supra* note 56.

[70] *Id*.

[71] Many of the ideas discussed in this section come from a prior article and are discussed in more depth there. *See* Camilla A. Hrdy. *Keeping ChatGPT a Trade Secret While Selling It Too*, BERKELEY TECH. L.J. (forthcoming 2025), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4879849

and explain why companies might choose to rely on trade secrecy along with, or in lieu of, patent and copyright law. I then assess whether trade secrecy protection can be successful for generative AI models sold publicly rather than used only in-house. I conclude by flagging the risk of reverse engineering and the possibility of using contracts to strengthen trade secrecy protection for generative AI.

### *A. Types of Information that Qualify as Trade Secrets*

Precedents involving software suggest that trade secrecy will substantially protect certain aspects of generative AI models. Although the types of information at issue will vary tremendously depending on how an AI is developed and deployed, scholars such as Sharon Sandeen have identified several broad categories of information related to AI that qualify as trade secrets.[72] I discuss each category below as applied specifically to generative AI technology, such as large language models. Importantly, I discuss these trade secrets in much more detail elsewhere and cite relevant case law, so that the reader can see that analysis.[73]

#### 1. Algorithms

Algorithms are used to train generative AI models and are also used in the AI model's embedded software systems. Some algorithms are human-made. Some may be AI-generated. Algorithms are a "natural" trade secret. They are not generally revealed to end users and may not be comprehensible even to those who created them. Courts have frequently protected algorithms related to AI in the past.[74]

#### 2. Code

Generative AI, like software, relies in large part on code. Source code is a classic trade secret because it can be kept secret even after the software is made available to end users.

---

[72] *See* Sharon Sandeen & Tanya Aplin, *Trade Secrecy, Factual Secrecy and the Hype Surrounding AI*, *in* RESEARCH HANDBOOK ON INTELLECTUAL PROPERTY AND ARTIFICIAL INTELLIGENCE 442–59 (Abbott ed., 2022) (discussing how trade secrecy might protect some factually secret features of AI systems used in autonomous vehicles and credit scoring, such as algorithms and source code); *see also* QUINN EMANUEL, THE RISING IMPORTANCE OF TRADE SECRET PROTECTION FOR AI-RELATED INTELLECTUAL PROPERTY (2020), https://www.quinnemanuel.com/the-firm/publications/the-rising-importance-of-trade-secret-protection-for-ai-related-intellectual-property/ [https://perma.cc/MJL6-2FFA] [hereafter *QUINN*] (discussing trade secrecy for AI-related technology); Gregory Gerard Greer, *Artificial Intelligence and Trade Secret Law*, 21 UIC REV. INTELL. PROP. L. J. 252 (2022) (discussing the degree to which trade secret law provides an alternative to patents for protecting AI); Ana Nordberg, *Trade Secrets, Big Data and Artificial Intelligence Innovation: a Legal Oxymoron?, in* THE HARMONIZATION AND PROTECTION OF TRADE SECRETS IN THE EU: AN APPRAISAL OF THE EU DIRECTIVE (Jens Schovsbo et al. eds., 2020) (exploring the scope of trade secret protection for AI); Sarah Speight, *Protecting Artificial Intelligence Via Trade Secrets*, WORLD INTELL. PROP. REV. (Sept. 1, 2023), https://www.worldipreview.com/rankings/global-trade-secrets/protecting-artificial-intelligence-via-trade-secrets [https://perma.cc/2NWQ-BTD8] (discussing trade secrecy protection for AI).

[73] *See* Camilla A. Hrdy. *Keeping ChatGPT a Trade Secret While Selling It Too*, BERKELEY TECH. L.J. (forthcoming 2025), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4879849

[74] *See, e.g.,* Glover v. Imubit, Inc., No. 2018-9003, 2019 Tex. Dist. LEXIS 72440, *1-2 (Jan. 14, 2019) (granting "emergency" temporary restraining order against plaintiff's former employee, after the court found the plaintiff would likely prevail in proving it owned trade secrets in "processes, procedures, algorithms, and technologies relating to artificial intelligence and machine learning . . . ."). *See also* Neural Magic, Inc. v. Meta Platforms, Inc., 659 F. Supp. 3d 138, 168 (D. Mass. 2023) (finding algorithms were identified with sufficient particularity when they were discussed in "detail" and "accompanied by diagrams, demonstrating their functions.").

Companies can sell software in a way that only reveals the "object code" or "executable code." Object code can only be read by machines. The source code, which can be read by human coders, is not revealed to users. The object code can be "decompiled" to reveal the source code. But this has historically been hard, costly, and time-consuming so courts have held the source code is still a trade secret even after the software is sold.[75] Thus, source code can be kept as a trade secret, even if the object code is not.[76] Companies can also rely on copyright law to protect source code. But trade secret claims will not generally be preempted so long as there is an additional allegation besides copying, such as breach of a duty or using improper means to acquire the source code. [77] I discuss the comparative limitations of copyright protection further below.

### 3. Training Data

Generative AI's most important trade secrets may be the training data that is used to train the models. This could include the training data itself, and also information regarding which training data was used, or which training data should be used, to train a model. As Andrew Torrence and Bill Tomlinson put it, "training is everything." They write:

> [Generative AI's] rely on large amounts of data to 'learn' how to perform tasks and make decisions. This data, referred to as 'training data,' is used to train AI algorithms to recognize patterns and make predictions based on those patterns. The accuracy of the AI algorithm is directly dependent on the quality and quantity of the training data that it is exposed to.[78]

Identifying, collecting, and obtaining permissions for training data can be extremely costly.[79] Keeping training datasets secret is likely to provide developers of generative AI with a major economic advantage over would-be competitors. Likewise, information about precisely

---

[75] *See* Sonia K. Katyal, *The Paradox of Source Code Secrecy*, 104 CORNELL L. REV.. 1183, 1229-1239 (asserting that it is "well settled" among courts that even wide distribution of software programs does not compromise trade secrecy so long as the program is not "readily ascertainable" and arguing that software code is not readily ascertainable because the source code remains "unpublished" while only the "object code" is revealed). *See also*, e.g., Fabkom, Inc. v. R.W. Smith & Associates, Inc., No. 95 Civ. 4552, 1996 WL 531873, at *3-4, *7-9 (S.D.N.Y. 1996) (finding plaintiff took reasonable measures to preserve secrecy of "source code, and the architecture of its [software] system" because the software was "distributed to its customers only in its executable object code form" while the source code was "restricted to plaintiff's principals"; and because the plaintiff provided the software "to clients only after they have signed a confidentiality agreement.").

[76] That said, if the object code is *also* kept secret from users, then it can potentially be a trade secret. Trandes Corp. v. Guy F. Atkinson Co., 996 F.2d 655, 662-664, note 8 (4th Cir. 1993) (holding software source code was a trade secret and that object code was also a trade secret because whereas usually "the owner of trade secret computer software will maintain the secrecy of the source code but freely distribute the object code . . ." here the plaintiff "maintained the secrecy of the source code and the object code . . .").

[77] Computer Assocs. Int'l, Inc. v. Altai, Inc., 982 F.2d 693, 717-719 (2d Cir. 1992) (trade secret and copyright claims available for source code because the "defendant's breach of duty is the gravamen of such trade secret claims, and supplies the "extra element" that qualitatively distinguishes such trade secret causes of action from claims for copyright infringement that are based solely upon copying." ) (applying 17 U.S.C. § 301).

[78] Andrew Torrence & Bill Tomlinson, *Training Is Everything: Artificial Intelligence, Copyright, and Fair Training*, DICKINSON L. REV. 223, 242 (2023).

[79] Lee et al., *supra* note 10, at 39-40 ("[T]he process of training — from transforming these inputs into a trained model — is expensive. It requires a substantial investment of multiple resources: time, data storage, and computing power.").

which data was used or which datasets work best could be very valuable. Some training data is of course public, but this is not necessarily fatal to trade secrecy. An entire training dataset can still be protectable as a "combination" trade secret, even if specific pieces of that information are public or can be easily discerned.[80] Courts apply divergent standards for protecting combination secrets, but the general rule is that the whole combination must impart an economic advantage due to its secrecy.[81]

#### 4. The Overall System Architecture of Specific Generative AI.

A model's technical architecture can have several components, depending on which form of model it is and how it was developed.[82] When building a large language model, a "neural network" is typically used. A "neural network" is a computational model that, in a sense, mimics the human brain.[83] Building such a neural network entails an extraordinary number of choices—in particular, which "weight parameters" to use in determining the strength of the connections between the nodes.[84] Any of this information could be a trade secret, including what method was used to build a model or the weight parameters that were used, in whole or in part, to the extent it would be valuable to others.

### *B. The Shortcomings of Patent Law in AI Protection*

One might think patents would be the natural option for protecting generative AI—especially those that will be publicly distributed. Unlike trade secrecy, a patent gives its owner the right to stop literally anyone from making, using, or selling the invention in the United States for a period of roughly twenty years. Independent development and reverse engineering are not allowed.[85]

Trade secret law, in contrast, only prohibits acts of misappropriation. It does *not* prohibit reverse engineering or independent development. These caveats significantly limit the universe of potential defendants in a trade secret case as compared to a patent case. There are usually only a few plausible categories of trade secret defendants: (1) current or former employees, as well as third parties who hire those former employees; (2) business partners, vendors, suppliers, and others who obtain trade secrets while under a legally-cognizable duty of confidentiality to the trade secret owner, as well as third parties with whom this information is shared; and (3) anyone who obtains trade secrets using "improper means."

---

[80] 18 U.S.C. § 1839 (3) (2016) (specifying that trade secrets can encompass information such as "compilations.").

[81] *See, e.g.*, Catalyst & Chem. Servs., Inc. v. Glob. Ground Support, 350 F. Supp. 2d 1, 8-10 (D.D.C. 2004) (citing Penalty Kick Mgmt. Ltd. v. Coca Cola Co., 318 F.3d 1284, 1291 (11th Cir. 2003) (applying District of Columbia UTSA) ("A combination qualifies as a trade secret only when there is an added value to the combination over the value of the individual parameters, *i.e.*, when 'the whole is more than the sum of the parts.'"), *aff'd*, 173 F. App'x. 825 (Fed Cir. 2006).

[82] Lee et al., *supra* note 10, at 11-12.

[83] *Id.* at 10-12; Tschider, *supra* note 10, at 689-91.

[84] Lee et al., *supra* note 10, at 11-12.

[85] *See* 35 U.S.C. § 154(a).

This third category of defendants can include *outsiders* with no prior relationship to the trade secret owner. But, for that sort of claim to work, the plaintiff has to identify an act that qualifies as an "improper means." As noted above in Part I, and discussed further below, this can potentially include so-called "hacking" by using automated or AI-assisted methods to access trade secrets. But it cannot include legal "reverse engineering," because under federal law "improper means" "does not include reverse engineering[.]"[86]

Trade secrecy's limitations make patents seem, initially, like a very attractive option. However, generative AI companies will likely choose to rely heavily on trade secrecy. There are many reasons for this preference.[87] One reason is that some aspects of generative AI are simply not patentable.[88] Commentators have flagged several patent eligibility problems. First, the "abstract idea" bar might preclude protection for a simple algorithm, or for an AI that merely automates a pre-existing process.[89] Second, patent law's disclosure and "enablement" requirements may present a challenge for patenting algorithms that are constantly evolving or whose operations human creators may not comprehend.[90] Third, increasing amounts of prior art is likely to render a lot of AI inventions non-novel or obvious.[91] Finally, there is a unique barrier to patenting the inventive outputs of generative AI because, at present, a purely AI-generated invention cannot be patented if it was not created by a human being.[92] Thus, while AI-related inventions developed by a human with help from AI may still be patentable,[93] it will likely be hard to patent AI-related inventions for which there is no identifiable human inventor.

To be clear, some generative AI inventions might be patentable. Examples might include a series of complex algorithms that yield specific technological improvements, a truly novel model architecture, or the software user interface.[94] But there are still other good reasons to prefer trade

---

[86] 18 U.S.C. § 1839(6); *see also* UTSA § 1, cmt.

[87] *See* J. Jonas Anderson, *Secret Inventions*, 26 BERKELEY TECH. L.J. 917, 956-60 (2011) (discussing the main factors that are likely to affect the private choice between patent and trade secrecy).

[88] QUINN, *supra* note 66, , at 1 ("Due to the prohibition on patenting abstract ideas . . . companies are increasingly turning to trade secret protection to protect their AI-related intellectual property.").

[89] *See* USPTO VIEWS, *supra* note 51; Matthew Hutson, *AI for Drug Discovery is Booming, but Who Owns the Patents?*, 41 NATURE BIOTECHNOLOGY 1494, 1494-95 (2023) (noting that while "there are close to 20,000 AI patents" an algorithm is "hard to patent" because "courts have often seen it as an abstract idea.").

[90] W. Keith Robinson, *Enabling Artificial Intelligence*, 60 HOUS. L. REV. 331 (2022) (discussing whether enablement poses significant challenge to the patenting of AI inventions and concluding that there is no need to modify enablement for AI).

[91] *See, e.g.*, Alex Baldwin, *Patenting AI: the IP Office Perspective*, WORLD INTELL. PROP. REV., Apr. 21, 2021, https://www.worldipreview.com/patent/patenting-ai-the-ip-office-perspective-21287 [https://perma.cc/UP5Z-JBFT].

[92] *See* Thaler v. Vidal, 43 F.4th 1207 (Fed. Cir. 2022); Ryan Abbott, *Artificial Intelligence and Intellectual Property: An Introduction, in* RESEARCH HANDBOOK ON INTELLECTUAL PROPERTY AND ARTIFICIAL INTELLIGENCE 2 (Ryan Abbott ed., 2022) (noting that at present, purely AI-generated inventions cannot be protected using either patent or copyright law to the extent that a non-human entity is the "inventor" for patent purposes or the "author" for copyright purposes).

[93] USPTO VIEWS, *supra* note 51, at 2-3 (explaining view that patentability is generally available for certain AI inventions).

[94] *See, e.g.*, Steven Kelly & Marla De Icaza, *The Story of AI in Patents*, WORLD INTELL. PROP. ORG. (Jan. 31, 2019), https://www.wipo.int/web/technology-trends/artificial_intelligence/story [https://perma.cc/FHK8-LFHC] (noting that the patent office has issued many generative AI patents already).

secrecy for certain information. First and foremost, as discussed in the prior section, many features of generative AI can be kept factually secret. They are hidden from users and are thus naturally conducive to secrecy. Indeed, some scholars opine that AI-based inventions are even more conducive to secrecy than traditional software. They "are even more difficult to reverse engineer because they are neither explainable nor scrutable."[95] Second, patents require extensive disclosure to the public, and companies may not want to disclose the "secret sauce" they used to develop a new generative AI—such as the specific data they collected to train the model.[96] Finally, the term length of a patent is limited to twenty years, whereas trade secrecy protection lasts so long as the information continues to derive economic value from secrecy and is the subject of reasonable secrecy measures.[97]

In the end, the calculus will likely look a lot like it did for software, where companies have often opted for trade secrecy over patenting for hidden information like source code and algorithms.[98] Thus, trade secrecy is and will continue to be a crucial way for companies to protect generative AI.[99]

### *C. Copyright's Comparative Limitations*

Companies can concurrently rely on copyright law to protect certain aspects of generative AIs, such as the source code and at least some of their training data. Although copyright law, unlike trade secret law, can protect publicly disclosed information, copyright law will not provide comprehensive protection. Companies will likely rely on trade secret law as well. Courts have held that companies can bring *both* copyright and trade secret claims to protect source code so long as there is an additional allegation besides unauthorized reproduction of copyrighted materials, such as breach of a duty or using improper means to acquire information.[100] There are two important categories of information related to generative AIs that will likely benefit from both trade secrecy and copyright protection.

Copyright law can be used to prohibit others from copying source code utilized in implementing generative AI or related software, assuming the code is sufficiently original and

---

[95] *See, e.g.,* Tabrez Y. Ebrahim, *Artificial Intelligence Inventions and Patent Disclosure*, 125 PA. ST. L. REV. 147, 184 (2020).

[96] *See* Mehdi Poursoltani, *Disclosing AI inventions*, 29 TEX. INTELL. PROP. L.J. 41, 56-57 (2021). *But see* Brian J. Love & Christopher B. Seaman, *Best Mode Trade Secrets*, 15 YALE J.L. & TECH. 1 (2012) (arguing that weakening of best mode requirement leaves option to obtain patents and also rely on trade secrets by keeping preferred mode of operation or manufacture secret).

[97] *See* QUINN, *supra* note 66, at 2.

[98] *Cf.* Katyal, *supra* note 69, at 1212-16 (discussing the choice between patent and trade secret with respect to software code and arguing that factors such as term length, conduciveness to secrecy, and costs of patenting shifted the balance towards trade secrecy for software)*; see also* QUINN, *supra* note 66*,* at 1 (discussing AI's amenability to trade secrecy).

[99] *See* QUINN, *supra* note 66, at 1.

[100] *See, e.g.*, Katyal, *supra* note 69, at 1207-08, 1228; Daryl Lim, *AI & IP: Innovation & Creativity in an Age of Accelerated Change*, 52 AKRON L. REV. 813, 835 (2018); *see also* Comput. Assocs. Int'l, Inc. v. Altai, Inc., 982 F.2d 693, 717-19 (2d Cir. 1992) (holding 17 U.S.C. § 301 did not preempt trade secret claim).

subject to the boundaries of fair use.[101] That said, a trade secret claim is actually more powerful than a copyright claim for protecting source code, at least to the extent the code is kept secret and has been the subject of misappropriation (i.e., used or disclosed in breach of a duty or acquired by improper means). The reason is that copyright law only protects "substantially similar" iterations of the code, and also includes a fair use outline. Trade secret law has neither of these limitations.

As Deepa Varadarajan has observed in her work, trade secret law is in some ways more powerful than copyright law. It protects the information writ large, regardless of whether the defendant's end product is different from the information obtained from the plaintiff,[102] and trade secret law contains no fair use defense.[103] This means that if someone obtains access to trade secret source code—whether through their employment or as an end user through a product—they can copy the information to make a completely new product for any purpose, yet still be liable under trade secret law.

It is also possible that copyright law will protect some training data as a compilation under copyright law. Copyright law protects for "compilations" of data.[104] Individual facts within a compilation are not protectable under copyright, but the overall arrangement and selection can be.[105] In theory, to quote Katherine Lee, A. Feder Cooper, and James Grimmelmann, training datasets "may be copyrightable as compilations, 'formed by the collection and assembling of preexisting materials or of data.' A compilation is copyrightable (separately from any copyright in the works it is assembled from) when the compilation itself features a sufficiently original 'selection or arrangement.'"[106] However, this protection will likely be limited to the compilation as a whole, and not include individual parts that are in themselves unprotectable. [107] In addition, as just mentioned, copyright would not prevent copying training data to make a substantially different end product.

### *D. The Success of Trade Secrecy Will Depend On How The Model Is Deployed*

The success of trade secrecy will largely depend on how the model is deployed. It will be easier to protect generative AI under trade secret law if a company uses it only in-house, and harder to protect models that are publicly-distributed, as ChatGPT is.

---

[101] *See* 17 U.S.C. § 101-02 (defining literary work in a way that includes computer code); *see also, e.g.*, Katyal, *supra* note 69, at 1198-1201 (discussing rise of copyright protection for code); Google LLC v. Oracle Am., Inc., 141 S. Ct. 1183 (2021) (fair use for software APIs).

[102] *See, e.g.*, Joseph P. Fishman & Deepa Varadarajan, *Similar Secrets*, 167 U. PA. L. REV. 1051, 1056-57 (2019).

[103] Deepa Varadarajan, *Trade Secret Fair Use*, 83 FORDHAM L. REV. 1401 (2014).

[104] *See* 17 U.S.C. § 101 ("A 'compilation' is a work formed by the collection and assembling of preexisting materials or of data that are selected, coordinated, or arranged in such a way that the resulting work as a whole constitutes an original work of authorship.").

[105] Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 345, 349 (1991).

[106] Lee et al., *supra* note 10*,* at 58 (citations omitted); *see also* Thomson Reuters Enter. Ctr. GmbH v. Ross Intelligence Inc., 694 F. Supp. 3d 467, 477 (D. Del. 2023). (recognizing compilation protection for whole database of judicial opinions including selection and arrangement, and suggesting defendant might be liable for training its own AI on this whole compilation).

[107] *See, e.g.,* Charles Tait Graves, The Part for the Whole In Trade Secret Law 4 (Feb. 13, 2024) (unpublished comment) (arguing that courts over-protect combination trade secrets by permitting causes of action based on using or disclosing only part of a combination trade secret).

Some businesses will surely develop—or license from others—generative AI tools for their own internal use.[108] Indeed, this is currently happening at a rapid pace and at a significant scale. Many companies are already replacing jobs done by human workers with generative AI tools.[109] As I write, major banks and investment companies are apparently considering replaying entry-level analysts with AI, "with as many as two-thirds of these positions potentially on the chopping block. This anticipated move could completely transform how these companies hire new employees and how they manage and deliver the technology employees use."[110]

From a trade secrecy perspective, when AI is deployed internally in lieu of human workers, this makes retaining trade secrecy in the AI tools a standard information management challenge. The company must use the usual security precautions—passwords and other digital safeguards—and have everyone who encounters the tools sign confidentiality agreements. This is how software is deployed internally already. Moreover, as Fromer has insightfully observed, when companies replace human workers with AI tools, this makes trade secrecy protection easier across the board. As explained above, companies that deploy AI can effectively replace their potentially disloyal, unreliable human workforce with loyal, predictable AI tools. These so-called "Oompa Loompas" (to use Fromer's term) are much more likely to keep the companies' trade secrets than humans, who would have potentially left the company and taken information with them.[111] This insight should logically apply both to companies' non-AI trade secrets and to the AI tools themselves.

In contrast, other companies will choose to sell or license their generative AI tools to others. There are many reasons to do this, including the desire to earn profits from sales and licensing, as well as the desire to train the AI on users' data. OpenAI, for example, distributes ChatGPT to the general public in various ways and already has millions of paying and non-paying users.[112] OpenAI also offers an Enterprise License, which lets businesses and developers access a more private, customized version of ChatGPT and also provides access to ChatGPT's application programming interface (APIs) to integrate ChatGPT into third-party apps.[113] Each day more players, including Google, Microsoft, and Meta, are training their own models and making them available to users.

---

[108] *See, e.g.,* Andrew McAfee, et al., *How to Capitalize on AI: A guide to realizing its benefits while limiting its risks*, HARVARD BUSINESS REVIEW (Nov.-Dec. 2023), https://hbr.org/2023/11/how-to-capitalize-on-generative-ai [https://perma.cc/X7CR-CXUX] (advising businesses on when and how to adopt generative AI in to improve operations).

[109] Kyt Dotson, *Cisco, IBM, Accenture and others join forces to address AI's impact on the workforce*, SILICONANGLE (Apr. 4, 2024, 12:55 PM), https://siliconangle.com/2024/04/04/cisco-ibm-accenture-others-join-forces-address-ais-impact-workforce/ [https://perma.cc/CAG4-J249].

[110] Elizabeth Montalbano, *AI poised to replace entry-level positions at large financial institutions*, CIO (Apr. 12, 2024), https://www.cio.com/article/2089550/ai-poised-to-replace-entry-level-positions-at-large-financial-institutions.html [https://perma.cc/BW5D-H6PE].

[111] Fromer, *supra* note 61, at 725.

[112] Peter Henderson et al. *Foundation Models and Fair Use* 4 (Stan. L. Sch. Working Paper Series, Paper No. 584), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4404340 [https://perma.cc/N9MK-76C7] ("Millions of users now use foundation model products. ChatGPT, a generalist chatbot from OpenAI, has grown to an estimated 100M daily active users.").

[113] Marty Swant, *With developer APIs for ChatGPT and Whisper, OpenAI is opening the floodgates with a familiar playbook*, DIGIDAY (Mar. 3, 2023), https://digiday.com/media-buying/with-developer-apis-for-chatgpt-and-whisper-openai-is-opening-the-floodgates-with-a-familiar-playbook/ [https://perma.cc/3WP3-VE2F].

Can publicly distributed generative AI tools be protected through trade secret law, even though millions of users have access to these tools? Precedents involving software indicate that the answer is *yes*. With software, companies have been able to protect trade secrets in the hidden features of their software that have not been fully disclosed to users. The main example is, of course, *source code*. Courts have held that source code can be a trade secret, under the assumption that decompiling source code is at present time-consuming and difficult.[114] Even though the process of discerning source code has gotten easier,[115] courts, in general, hold that code is a trade secret so long as it's not fully revealed to users.[116]

As with software, generative AI companies can distribute their generative AI models in ways that do not reveal all the information needed to replicate it. As Katherine Lee, A. Feder Cooper and James Grimmelmann have observed, many generative AI companies distribute their models in ways that hide the model's inner workings from users. In fact, most users are not given access to the "model" at all. They only interact with the user interface, which is technically a separate software system from underlying generative AI technology.[117] ChatGPT users, for example, generally have no idea how the underlying generative AI models work or how it reached its conclusions. From users' viewpoint, ChatGPT is merely a "chatbot" that generates responses to their queries.

### *E. The Risk of Reverse Engineering*

The major caveat to relying on trade secrecy, as opposed to patent law, is that "reverse engineering" remains legal. Recall that in trade secret law there must be an act of misappropriation, which does not include reverse engineering. The term "reverse engineering" generally means discerning otherwise secret information from a product or service available on the open market by observing it, picking it apart, doing tests on it, decompiling source code, etcetera.[118]

At present, reverse engineering generative AI technology based only on public access is probably impossible. However, reverse engineering typically gets easier and cheaper over time.

---

[114] *See, e.g.,* Sonia K. Katyal, *The Paradox of Source Code Secrecy*, 104 CORNELL L. REV. 1183, 1195-1203 (2019); Mark A. Lemley*, Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239, 1243-1244 (1995).

[115] Samuel J. LaRoque, *Reverse Engineering and Trade Secrets in the Post-Alice World*, 66 KAN. L. REV. 427, 438-439 (2017).

[116] *Compare* NEXT Payment Sols., Inc. v. CLEAResults Consulting, Inc., No. 17 C 8829, 2018 WL 3637356, at *13 (N.D. Ill. July 31, 2018) (finding computer software was a trade secret where it was confidential and plaintiffs "derived economic value from [its software] not being generally known or accessible."), *with* Arkeyo, LLC v. Cummins Allison Corp., 342 F. Supp. 3d 622, 630 (E.D. Pa. 2017) (plaintiff lost trade secrecy in software when it left a zip file on the internet that "contained mostly executable code" rather than "human readable source code," because the executable code "could be translated into source code through the relatively simple process of decompilation—a process as simple as translating French into English.").

[117] Lee et al., *supra* note 10, at 41-42 (discussing "closed source" generative AI models). *See* discussion in Part I *supra*.

[118] Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L. J. 1575, 1577 (2002) (defining reverse engineering broadly as "the process of extracting know-how or knowledge from a human-made artifact.").

Once reverse engineering a publicly accessible product or service becomes possible, this has two consequences for trade secrecy.

First, the person doing the reverse engineering is not liable—*assuming* the activities are deemed legal reverse engineering versus "improper means." That is an important assumption because, as mentioned above, case law like *Compulife* suggests that a court might deem something that appears to be reverse engineering "improper"—especially if it draws on automation or AI.

Second, trade secrecy rights can end altogether, even for insiders, because the information is deemed generally known or "readily ascertainable" through proper means—*assuming* reverse engineering is easy and not very expensive or time-consuming, and *assuming* the means of reverse engineering is deemed proper.

What does this mean for generative AI's trade secrets? It means that trade secrecy will end once reverse engineering becomes easy, quick, and inexpensive.[119] Take the example of ChatGPT. If it becomes possible to reverse engineer information regarding the underlying AI model by merely accessing the public chatbot interface, the person who did the reverse engineering would not be liable for trade secret misappropriation (assuming a court does not deem the methods improper). Over time, as reverse engineering gets cheaper and easier, this would *also* mean that ChatGPT's trade secrets—whichever aspects of them can be discerned through reverse engineering—would end as well. So even OpenAI employees could freely use that information outside the company. There are many caveats to this—in particular contracts. As discussed in the final part, contractual provisions are at play too. But still, purely as a matter of trade secret law, the risk of easy and cheap reverse engineering has significantly negative implications for trade secrets.

How could a generative AI model be reverse-engineered? One possible method is the "model extraction attack." A model extraction attack typically entails using a series of queries to an AI system, and analyzing the AI's responses to infer its underlying elements, such as overall architecture, how the model was developed and trained, and even some of the training data.[120] For example, model extraction attacks have been used to discern which training data was used to train an AI.[121]

We recently saw a high-profile example of someone trying to reverse engineer training data in the ongoing copyright litigation between the *New York Times* and OpenAI. The *Times* is arguing that Open AI used copyrighted *New York Times* content to train ChatGPT, and that

---

[119] *See* Sherkow, *supra* note 16, at 1078.

[120] Milad Nasr et al.,, *Scalable Extraction of Training Data from (Production) Language Models*, ARXIV 1 (2023) https://arxiv.org/abs/2311.17035 [https://perma.cc/WTF2-3JQ3] (asserting that through a technique called "extractable memorization," it is possible to "efficiently extract" "training data . . . by querying a machine learning model without prior knowledge of the training dataset."); *see also* Florian Tramèr et al.,, *Stealing Machine Learning Models via Prediction APIs*, *in* 25TH USENIX SECURITY SYMPOSIUM, USENIX SECURITY 601 (2016); *see also* Winograd, *supra* note 10, at 625–626 (discussing a "training data extraction attack" whereby an "adversary" "deliberately causes a model to leak memorized information" to extract users' private information). *See also* Devin P. Owens, Artificial Intelligence Models May Not Have Owners 3–6 (Sep. 22, 2024) (unpublished student paper) (on file with author).

[121] Matthew Sag, *Copyright Safety for Generative AI*, 61 HOUS. L. REV. 295, 326–327 (2023).

ChatGPT, upon prompting, will provide nearly-verbatim copies of *Times* articles. OpenAI claims that, in order to orchestrate this proof of copying, the *New York Times* hired someone to "hack" OpenAI's platforms and perform strategic prompting over thousands of attempts in order to elicit the most responses the *Times* wanted. OpenAI also alleges that these actions were taken in violation of OpenAI's terms of use, an issue I discuss in the next section.[122]

More recently, OpenAI accused the makers of the new AI model, "DeepSeek," of engaging in "knowledge distillation" to develop their system. Knowledge distillation is a technique where a smaller model is trained to replicate the behavior of a larger, more complex model by learning from its outputs. OpenAI alleges that DeepSeek used this method to extract information from OpenAI's models, potentially violating their terms of service. DeepSeek has denied these allegations, asserting that their model was developed independently. [123]

Reverse engineering techniques, such as model extraction attacks and knowledge distillation, will inevitably continue to improve. Courts will have to decide whether these activities violate trade secret law and whether reverse engineering has become so simple that trade secrets have been destroyed. In both of the situations above—model extraction and knowledge distillation—OpenAI could argue the actors are liable for trade secret misappropriation.

There are several ways to make the argument that using model extraction attacks or knowledge distillation constitutes acquisition of trade secrets by "improper means." First, even though, all else being equal, reverse engineering is legal under trade secret law, using "improper means" to acquire trade secrets is not. As discussed above, case law like *Compulife* suggests that using automated, non-human methods to acquire trade secrets can constitute "improper means" rather than legal reverse engineering. Courts may well view these newer methods to be "improper," just as the court in *CompuLife* viewed data scraping to be "improper."[124] If so, then using these new methods to "hack" generative AI's would be misappropriation.

Second, as discussed below, contractual prohibitions, such anti-reverse-engineering clauses, can enhance protection under both trade secret and contract law. The reason is that courts

---

122 "The truth, which will come out in the course of this case, is that the Times paid someone to hack OpenAI's products. It took them tens of thousands of attempts to generate the highly anomalous results that make up Exhibit J to the Complaint. They were able to do so only by targeting and exploiting a bug (which OpenAI has committed to addressing) by using deceptive prompts that blatantly violate OpenAI's terms of use." Complaint at 2, The New York Times Company v. Microsoft Corporation et al, No. 1:23-cv-11195, (S.D.N.Y. Dec. 12, 2023).

123. *See, e.g.,* OpenAI Accuses Chinese Startup DeepSeek of Unauthorized Data Use, Sparking AI Ethics Debate, THE OUTPOST AI, Jan. 31, 2025, 3:02 AM, https://www.theoutpost.com; Houman Asefi, "The OpenAI vs DeepSeek Knowledge Distillation Dispute: Technical and Legal Implications," MEDIUM, Jan. 30, 2025, https://houman-asefi.medium.com/the-openai-vs-deepseek-knowledge-distillation-dispute-technical-and-legal-implications-1e69d646b928; John Werner, "Did DeepSeek Copy Off Of OpenAI? And What Is Distillation?" FORBES, Jan. 30, 2025, https://www.forbes.com/sites/johnwerner/2025/01/30/did-deepseek-copy-off-of-openai-and-what-is-distillation/

124 *See* Compulife Software, Inc. v. Newman, 111 F.4th 1147, 1162-1163 (11th Cir. 2024) (affirming holding that using automated robot to collect data from website was improper means). It is important to note that the Eleventh Circuit opined that the defendants' actions were particularly bad because "they copied the order of Compulife's copyrighted code and used that code to commit a scraping attack…" *Id*. at 1162-63. The court noted that in some situations "scraping and related technologies (like crawling) may be perfectly legitimate." *Id*. at 1162-63. Thank you to Victoria Cundiff for this astute insight about the Eleventh Circuit's opinion.

tend to view acquisition of trade secrets as more "improper" when they are expressly addressed and prohibited through a contract. Put differently, when generative AI companies like OpenAI prohibit using their models to discern trade secrets, this helps ensure that using generative AI to discern trade secrets will be deemed illegal under trade secret law. In *Compulife*, the plaintiff's website did *not* initially have a terms of use restrict users' ability to employ automated means to access information from the plaintiff's website.[125] (That said, notably, Compulife added new terms of use to its website after it learned of defendants' activities, presumably in order to make it clear in the future that such attacks were contractually prohibited.)[126]

### *F. Contracts will enhance legal protection for generative AI.*

To the extent reverse engineering does become feasible, generative AI companies can use contracts to shore up, and go beyond, trade secrecy protection—just as companies have done for traditional software. With software, companies enhanced legal protection for their products by structuring sales of the software as "licenses" and attaching "end user license agreements" (EULAs) or "terms of use," which significantly limit what users can do with the software.[127]

Like traditional software, generative AI models are licensed, not sold, to users. Users typically agree to terms of use or end-user license agreements before signing up. For example, ChatGPT users must agree to OpenAI's terms of use.[128]

OpenAI's terms of use, which are similar to others I've seen, contain three provisions that are particularly relevant to trade secrecy protection. Below I explain how each of these provisions might strengthen trade secrecy protection for the underlying models.

#### 1. Anti-Reverse-Engineering Provisions

First, generative AI users will likely have to agree to a provision prohibiting "reverse engineering" of the model to learn its secrets or replicate its functionality. Open AI's terms of use prohibits attempting to "reverse engineer, decompile or discover the source code or underlying components of our Services, including our models, algorithms, or systems …" and specifically prohibits attempting to "[a]utomatically or programmatically extract data or Output" from ChatGPT.[129]

---

125. *See* Compulife Software, Inc. v. Rutstein, No. 9:16-CV-80808-JMH, 2018 WL 11033483, at *19 (S.D. Fla. Mar. 12, 2018).

126. Compulife Software, Inc. v. Rutstein, No. 9:16-CV-80808, 2021 WL 3713173, at *10 (S.D. Fla. July 12, 2021).

127 *See* Lemley, *supra* note 107, at 1243-45.

128 *Terms of Use*, *supra* note 34. Enterprise License users must agree to separate Business Terms. *See Business Terms, supra* note 33.

129 *Terms of Use*, *supra* note 34.

Reverse engineering is legal under trade secret law, but it can be prohibited through contract law. Anti-reverse engineering are typically enforced as a matter of contract law.[130] Preemption challenges based on copyright law have not gotten very far as of yet.[131] What is not as obvious is that obtaining trade secrets in breach of an anti-reverse engineering clause can be deemed misappropriation of trade secrets. This may seem surprising because reverse engineering is legal under trade secret law. However, some courts have held that reverse engineering a product in violation of an anti-reverse engineering clause can itself constitute "improper means" and thus trade secret misappropriation—even if the anti-reverse engineering clause appears in a non-negotiated terms of use or end user license agreement (EULA) that is attached to publicly-distributed software.[132]

Courts could apply this same reasoning to generative AI. If a company or individual reverse engineers a generative AI model in breach of a terms of use or EULA that broadly prohibits reverse engineering—or even specifically prohibits the means used—then the AI company can sue for trade secret misappropriation, as well as breach of contract. If successful, the AI company can get trade secret law remedies, not just contract law remedies. This would include monetary and injunctive relief. Moreover, third parties who knowingly obtain reverse-engineered information from a licensee could also potentially be liable.[133]

---

[130] *See, e.g.,* Bowers v. Baystate Techs., Inc., 320 F.3d 1317, 1324-26 (Fed. Cir. 2003) ("[P]rivate parties are free to contractually forego the limited ability to reverse engineer a software product under the exemptions of the Copyright Act) (citing, *e.g.,* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 39 USPQ2d 1161 (7th Cir.1996)). *See also, e.g.,* Meridian Project Sys., Inc. v. Hardin Const. Co., LLC, 426 F. Supp. 2d 1101, 1107 (E.D. Cal. 2006) (enforcing anti-reverse engineering clause in the End User License Agreement (EULA) finding this was not "an unconscionable contract or a contract of adhesion."); Triage Logic Mgmt. & Consulting, LLC v. Innovative Triage Servs., LLC, No. 20 CVS 399, 2020 WL 4597279, at *7 (N.C. Super. Aug. 11, 2020) (enforcing clause that prohibited Defendant from "modify[ing], disassembl[ing], decompiling, reverse engineer[ing] or otherwise re-creat[ing] [Plaintiff's software system], in whole or in part.") (citing Sparrow Sys., Inc. v. Priv. Diagnostic Clinic, PLLC, No. 14 CVS 1025, 2014 WL 7592501, at *7 (N.C. Super. Dec. 24, 2014) (enforcing clause stating that "[Defendant] agrees that, without [Plaintiff's] prior written consent, [Plaintiff's] Software shall not be ... translated, decompiled or disassembled by reverse engineering or otherwise adapted in any way.")).

[131] *See* cases cited in note 130 *supra*. *See generally* Guy Rub, *Copyright Survives: Rethinking the Copyright-Contract Conflict*, 103 VIRGINIA LAW REVIEW 1141, 1147 (2017) (observing increasing dominance of the "no-preemption" approach that allows contracts to go beyond copyright). *See also, e.g.*, Yang Chen, *Enforceability of Anti-Reverse Engineering Clauses in Software Licensing Agreements: The Chinese Position and Lessons from The United States and European Union's Laws*, 43 U. PA. J. INT'L L. 783, 803-804 (2022) (discussing case law regarding enforceability of anti-reverse engineering clauses under U.S. copyright law). *But see* Mark A. Lemley & Peter Henderson, *The Mirage of Artificial Intelligence Terms of Use Restrictions*, Princeton University Program in Law & Public Affairs Research Paper No. 2025-04, 10 Jan 2025, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5049562 (arguing that many of the AI companies' terms of use should be preempted by copyright law and that courts may begin turning away from the no-preemption approach).

[132] *See, e.g.,* Socal Diesel, Inc. v. Extrasensory Software, Inc., No. B290062, 2022 WL 702427, at *9 (Cal. Ct. App. Mar. 9, 2022), reh'g denied (Apr. 8, 2022) (holding that if the end user of software has "agreed to the EULA—which specifically prohibited reverse engineering—with the intention of breaching it, that would constitute an improper means of obtaining [plaintiff's] trade secret."). *But see* Aqua Connect, Inc.v. Code Rebel, LLC, No. CV 11-5764-RSWL MANX, 2012 WL 469737, at *2 (C.D. Cal. Feb. 13, 2012) (citing DVD Copy Control Ass'n, Inc. v. Bunner, 31 Cal.4th 864, 901 (2003) (Moreno, J., concurring) ("[N]owhere has it been recognized that a party wishing to protect proprietary information may employ a consumer form contract to, in effect, change the statutory definition of 'improper means' under trade secret law to include reverse engineering, so that an alleged trade secret holder may bring an action."). *See also* Pamela Samuelson, *Reverse Engineering Under Siege*, 45 COMMC'N ACM 15, 17 (2002).

[133] Camilla A. Hrdy & Christopher B. Seaman, *Beyond Trade Secrecy: Confidentiality Agreements That Act Like Noncompetes*, 133 YALE L. J. 669, 687 (2023) (contrasting contract and trade secret remedies).

### 2. Noncompete Provisions

Second, users of a generative AI model may have to sign a noncompete agreement. A noncompete agreement, also called a "noncompete," is a contract that prohibits competition, usually for a limited period of time. Based on statutory or common law, workplace noncompetes are unenforceable in some states, such as California; and in all states, noncompetes are subject to at least the requirement that they be "reasonable."[134] A noncompete must be "reasonable" in terms of its duration and geographic reach, and in terms of the scope of competing activity it restricts; it also must be necessary to protect a "legitimate business interest," including but not limited to the need to protect trade secrets.[135]

A noncompete is an extreme form of protection that goes beyond what trade secret law alone can do. Whereas trade secret law prohibits using or disclosing a particular piece of information, noncompetes prohibit *competition*, regardless of whether certain information is used or not.[136] Noncompetes are extremely common in the workplace,[137] but AI companies are deploying them against end users. For example, users of OpenAI's ChatGPT are prohibited from using ChatGPT "Outputs" to develop any artificial intelligence "models that compete with Open AI."[138] Meta, which releases its Llama model in an "open-source" format that permits users to access the code and training data, also has a somewhat similar provision in its EULA, stating: "You will not use the Llama Materials or any output or results of the Llama Materials to improve any other large language model (excluding Llama 2 or derivative works thereof)."[139]

These provisions are likely to be interpreted as noncompetes because they restrict the ability of users to develop competing products. Their enforceability is highly uncertain. On the one hand, the ChatGPT and Meta clauses are unusual, because they are not total bars on competition. They state that users cannot use ChatGPT or Llama *outputs* to develop similar large language models that might compete with OpenAI or Meta, respectively.

However, they are likely to be found unenforceable, even under statutory or common law "reasonableness" standards, because they lack a time limit. They last forever. For example, I found a recent case saying exactly that for a software noncompete.[140] A North Carolina state court found a noncompete clause in a software license agreement to be an illegal restraint on trade and

---

134 *Id*. at 673-74.

135 *Id*. at 719 (citing Restatement (Second) of Contracts § 188).

136 *Id*. at 673-675 (comparing scope of a noncompete to scope of a confidentiality agreement or a trade secret claim).

137 *Id*. at 683.

138 *Terms of Use*, *supra* note 31, at 3 (limiting language in the Business Terms, applying to businesses and developers getting an Enterprise License, can be observed, and stating that the licensee cannot "use Output to develop any artificial intelligence models that compete with our products and services. However, you can use Output to (i) develop artificial intelligence models primarily intended to categorize, classify, or organize data (e.g., embeddings or classifiers), as long as such models are not distributed or made commercially available to third parties and (ii) fine tune models provided as part of our Services[.]"); *Business Terms, supra* note 30, at 3.

139 *Llama 2 Community License Agreement*, META (July 18, 2023), https://ai.meta.com/llama/license/ [https://perma.cc/K4GP-PF86].

140 Triage Logic Mgmt. & Consulting, LLC v. Innovative Triage Servs., LLC, No. 20 CVS 399, 2020 WL 4597279, at *8 (N.C. Super. Aug. 11, 2020).

unenforceable under North Carolina law. The clause provided that "the Licensee shall not . . . develop similar software, services or product offerings substantially similar to the System."[141] The court classified the clause as a noncompete, explaining that even if the contract did not use the words "do not compete," it was a restriction on competition and unenforceable under North Carolina law because it lacked a time limit.[142]

### 3. Confidentiality Provisions

Finally, those who pay for an "enterprise" license[143] will likely have to agree to a confidentiality agreement. Generative AI "enterprise" licenses are designed for companies that are willing and able to pay for broader access to a generative AI model, including with the right to use the model to develop their own derivative systems. Such an enterprise license will likely be governed by its own terms of use, and this terms of use may have a *confidentiality agreement*.[144]

A confidentiality agreement is a contract that prevents a party from using or disclosing any information that the contract defines as "confidential." Confidentiality agreements are typically enforceable to the extent they cover information that is not publicly available. This can include trade secrets, as well as non-trade-secret information that is nonetheless non-public.[145] For example, a confidentiality agreement could protect algorithms that are kept reasonably secret, even if a court finds the algorithms fail to meet trade secret law's "independent economic value" requirement.

Along with generating contractual liability for those who use or disclose covered information, a confidentiality agreement is also important for ensuring that information can be protected under trade secret law. As mentioned above, trade secret law has two routes to liability. I have mostly discussed the "improper means" route—where an outsider acquires trade secrets using improper means. But trade secret law also generates liability for *insiders* who receive trade secrets under a duty of confidentiality, and use or disclose those trade secrets in breach of that duty. The plaintiff, in these cases, has no burden to show that the defendant used "improper means" to acquire the information.[146]

The upshot is that anyone who enters an "enterprise" license with a generative AI company, and agrees to a confidentiality agreement in that license, will be liable for breach of contract, *as*

---

[141] *Id.* at *2.

[142] *Id*. at *9..

[143] Notably, the terms of use that applies to ordinary users has no confidentiality agreement. The initial version did, but OpenAI removed it. I discuss this development in my forthcoming article.https://openai.com/enterprise *See* Camilla A. Hrdy. *Keeping ChatGPT a Trade Secret While Selling It Too*, BERKELEY TECH. L.J. (forthcoming 2025), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4879849

[144] For example, Open AI's "Business Terms," which applies to its enterprise licensees, are prohibited from using or disclosing Open AI's "Confidential Information." *See Business Terms, supra* note 33.

[145] Camilla A. Hrdy & Christopher B. Seaman, *Beyond Trade Secrecy: Confidentiality Agreements That Act Like Noncompetes*, 133 YALE L. J. 669, 750-751 (2023) (explaining categories of information that might qualify for protection under a confidentiality agreement even if they are not trade secrets).

[146] *See, e.g.*, ChampionX, LLC v. Resonance Sys., Inc., No. 3:21-CV-288-TAV-JEM, 2024 WL 1345698, at *12 (E.D. Tenn. Mar. 28, 2024) (distinguishing trade secret claims based the theory that defendant obtained information "via improper means" and the theory that the defendant used or disclosed information after receiving the information "under circumstances giving rise to a duty to maintain its secrecy or limit its use.").

*well as trade secret misappropriation,* if they thereafter use or disclose the generative AI company's trade secrets without authorization. This puts licensees in a somewhat similar situation to employees. They cannot use or share covered information, or they risk being sued for both trade secret misappropriation and breach of contract.

## CONCLUSION

I have pointed out three major issues that generative AI raises for trade secret law. This novel technology will inevitably push us to search for analogies from the past to decide how these legal issues will play out. Doing so will be especially important for trade secret law. Trade secret law has historically proceeded by the common law method. The statutes are sparse. Courts have significant discretion. Identifying analogies can at least help practitioners and academics locate case law where courts struggled in the past with similar issues.

The first issue I discussed is the new risk generative AI poses to companies' existing trade secrets and the alarming possibility that more and more information might be deemed "readily ascertainable" and thus unprotectable by trade secret law. This is similar to prior circumstances where rapid technological advances has threatened trade secrets by rendering previously-hidden information effectively public. The main example that comes to mind is the internet. But, there have been many past scenarios where a technological advance suddenly weakens trade secrecy, ranging from source code decomplication techniques to DNA sequencing methods.[147] These are areas that we can look to for case law guidance.

The second issue I discussed is whether AI-generated information can be protected as trade secrets, even if no humans are involved in the creation process. I argue that trade secret protection is possible. Not only does trade secret lack any affirmative human-creator requirement, but trade secret law has long shifted ownership of employee-generated inventions to the employer. If employee-created information can be owned by employers, and employee-created information is analogous to machine-generated information, this suggests that machine-generated information can be owned by employers, too. I also addressed complications raised by AI-generated information. For example, if the AI tool itself is widely available, does this mean any inventions derived from that tool are necessarily readily ascertainable and thus not protectable as trade secrets?

The final issue discussed is whether generative AI technology will itself be protectable under trade secret law. I argue the answer is, resoundingly, yes. However, the degree of protection will depend on how the technology is implemented and managed. For example, it will be much easier for companies to retain trade secrecy in generative AI tools used only in-house, within businesses. But even when AI tools are sold or licensed to the general public—as is the case with ChatGPT—companies will still be able to retain significant trade secrecy. The clearest analogy from past technology is software. For better or worse, case law involving software

[147] *See, e.g.,* Sherkow, *supra* note 16, at 1078(discussing advances in DNA sequencing technology that make it easier to discern DNA trade secrets); LaRoque, *supra* note 108, at 439 (discussing advances that make it easier to discern source code from object code).

strongly supports that information related to generative AI can retain its trade secret status so long as it is not fully revealed to users. Several types of information will likely qualify, including algorithms, source code, training data, and specific information regarding how an AI was trained, developed, or refined. Moreover, as with software, companies can use contracts—terms of use and EULAs—to obtain greater protection than that allowed by trade secret law alone. I discussed several types of contractual provisions already being used, including confidentiality, anti-reverse engineering, and noncompete provisions.

This landscape will continue to evolve as AI technology evolves. But I hope that I have provided a useful starting point to assess these issues.